

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

UNITED STATES OF AMERICA,

Case No. 22-CR-225 (NEB/DTS)

Plaintiff,

v.

ORDER ON REPORT AND
RECOMMENDATION

SHARMAKE JAMA, et al.,

Defendants.

In 2022, six individuals were indicted for their roles in an alleged scheme to defraud the Federal Child Nutrition Program. (ECF No. 1.) Five of the defendants—Sharmake Jama, Ayan Jama, Asha Jama, Mustafa Jama, and Zamzam Jama (“Defendants”)—jointly moved to suppress search warrant evidence and to dismiss for selective prosecution. (ECF Nos. 132, 135.) In a Report and Recommendation, United States Magistrate Judge David T. Schultz recommends denying both motions. (ECF No. 173 (“R&R”).) Sharmake Jama objects to the recommendation to deny the motion to suppress. (ECF No. 174.) Defendants object to the recommendation to deny the motion to dismiss. (ECF Nos. 175.) For the reasons below, the Court overrules the objections and denies the motions.

BACKGROUND

Judge Schultz's R&R sets forth an appropriate overview of the factual and procedural history. The Court will assume the parties are familiar with the background facts.

ANALYSIS

I. Legal Standard

The Court reviews the portions of the R&R to which Defendants object *de novo*. 28 U.S.C. § 636(b)(1); Fed. R. Crim. P. 59(b)(3).

II. Motion to Suppress Search Warrant Evidence

As part of its investigation, law enforcement obtained two search warrants for email accounts stored by Google and Microsoft that were connected to the Brava Restaurant. (ECF Nos. 133-1 (Google warrant), 133-2 (Microsoft warrant).) Defendants moved to suppress evidence gathered from these warrants, arguing that the warrants were overbroad and lacked particularity in violation of the Fourth Amendment. (ECF Nos. 132, 133.) Specifically, they challenge Attachments A and B to the warrant applications. Attachment A to each warrant application states that the "warrant applies to all information associated with" specific email accounts stored by Google and Microsoft, respectively. (ECF No. 133-1 at 34 (identifying five Google email accounts); ECF No. 133-2 at 34 (identifying three Microsoft email accounts).) Attachment B to the warrant applications appear identical, requiring the providers (Google and Microsoft) to

disclose information “for each account or identifier listed in Attachment A for the time period from January 1, 2020 to the present” including the “contents of all e-mails associated with the account.” (ECF No. 133-1 at 35; ECF No. 133-2 at 35.) Attachment B then enumerates 13 specific categories of information to be seized by the government. (ECF No. 133-1 at 36–38; ECF No. 133-2 at 36–38.)

The R&R recommends denying the motion to suppress. (R&R at 5–14.) Sharmake Jama objects to three aspects of the R&R: (1) the conclusion that the warrants were constitutionally sufficient; (2) the finding that Defendants’ relevant-timeframe critique lacks a factual basis; and (3) the conclusion that the *Leon*¹ good-faith exception applies. (ECF No. 174.) None of these objections has merit.

A. *Constitutional Sufficiency*

The motion to suppress contends that the search warrants failed to satisfy the Fourth Amendment’s mandate that “no Warrants shall issue . . . [unless] particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. Defendants’ motion relies in part on *United States v. Moulder*, No. 20-CR-232 (JRT/BRT), 2022 WL 3644893 (D. Minn. Aug. 24, 2022). (See ECF No. 133 at 8–10 (citing *Moulder* repeatedly).) In *Moulder*, a district court found that an “initial request for all records from Google fail[ed] the Fourth Amendment particularity requirements and [wa]s overbroad.” 2022 WL 3644893, at *4.

¹ *United States v. Leon*, 468 U.S. 897 (1984).

The R&R considered—and rejected—*Moulder's* rationale. (R&R at 6–12.) This Court also disagrees with *Moulder's* reasoning and recently concluded that *Moulder* was inapplicable to the search warrant of an email account in a related Feeding Our Future case. *See United States v. Bock*, No. 22-CR-223 (NEB/DTS), 2025 WL 18629, at *12–14 (D. Minn. Jan. 2, 2025) (rejecting *Moulder* and finding the warrant was sufficiently particular and not overbroad). In his objection, Sharmake Jama does not defend *Moulder*. He maintains that the R&R erred in claiming that Defendants relied solely on the *Moulder* argument.² Instead, he relies on “the plain text of the Fourth Amendment” and “the body of law against General Warrants” to argue that attachments to the warrant applications were not sufficiently particularized. (ECF No. 174 at 4; *see id.* at 3.)

The particularity requirement prohibits law enforcement “from conducting general, exploratory rummaging of a person’s belongings,” and requires that the warrant be “sufficiently definite to enable the searching officers to identify the property authorized to be seized.” *United States v. Shrum*, 59 F.4th 968, 973 (8th Cir. 2023) (citations omitted). This requirement is “one of practical accuracy rather than of hypertechnicality.” *Id.* (citation omitted). “Whether a warrant fails the particularity requirement cannot be decided in a vacuum. The court will base its determination on such factors as the purpose for which the warrant was issued, the nature of the items to which it is directed, and the

² The R&R states that Defendants relied “*almost exclusively*” on *Moulder*. (*See* R&R at 6 (emphasis added)).

total circumstances surrounding the case.” *United States v. Fiorito*, 640 F.3d 338, 346 (8th Cir. 2011) (citation omitted).

When the subject of a warrant is electronic information, Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure authorizes “a later review” of seized electronic information so long as that review is “consistent with the warrant.” Fed. R. Crim. P. 41(e)(2)(b); *see United States v. Schesso*, 730 F.3d 1040, 1046 n.3 (9th Cir. 2013) (noting Rule 41(e)(2)(b) “explicitly permits the seizure or copying of electronically stored information for later off-site review”). Because electronic devices “commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location,” Rule 41(e)(2)(b) “acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.”³ Fed. R. Crim. P. 41, advisory committee’s note to 2009 amendments.

And so, just because Attachment B requires Google or Microsoft to disclose the entire contents of email accounts (that were specifically identified in Attachment A) does not mean that law enforcement can search for anything in that disclosure. The search is

³ As noted in *Bock*, Courts of Appeal consistently understand Rule 41(e)(2)(b) to authorize off-site storage and later review of electronic information. 2025 WL 18629, at *13 & n.17 (collecting cases); (*see also* R&R at 7–8 (collecting cases that have found the two-step process constitutional).)

constrained by the preexisting warrant, which, of course, must satisfy particularity and breadth requirements. Here, “law enforcement discretion is constrained and limited to the items to be seized that are specified in Attachment B to the warrant.” *Matter of Search of Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc.*, 13 F. Supp. 3d 157, 164 (D.D.C. 2014) (granting search warrant application where the “government identifie[d] the precise location to be searched—[an] e-mail account—and specifie[d] in the attachments to its application the particular e-mails to be seized”). Defendants do not dispute that Attachment B’s 13 categories of information to be seized are sufficiently particular and linked directly to the alleged fraud scheme. (See ECF No. 133 at 8–9 (“‘Attachment B [section] II’ to the Affidavits are sufficiently particularized.”).)

For these reasons, the warrants were sufficiently particular and not overbroad. This objection is overruled.

B. Relevant Timeframe

Sharmake Jama next argues that the R&R mistakenly found that the warrants include a timeframe limitation. (See R&R at 12.) He argues that “*Attachment A contains no time or content restrictions whatsoever*,” and so the warrants were overbroad. (ECF No. 174 at 4.)

Jama acknowledges that Attachment B includes a date range and does not claim that the timeframe was unreasonable. (ECF No. 174 at 5 n.1.) In essence, he argues that

the warrants are overbroad because the timeframe identified in Attachment B was not identified in Attachment A. He cites no caselaw supporting this hypertechnical reading of a warrant application, and the Court is aware of none. *Cf. Fiorito*, 640 F.3d at 346 (“The particularity requirement ‘is a standard of practical accuracy rather than a hypertechnical one.’” (citation omitted)); *see generally United States v. Bieri*, 21 F.3d 811, 815 (8th Cir. 1994) (rejecting overbreadth argument and noting that courts are to “examine applications and affidavits for issuing a search warrant using a ‘common sense approach and not in a hypertechnical fashion’” (citation omitted)).

Attachment A identifies the email accounts to which the warrants apply; it does not order Google and Microsoft to *disclose* all records, files, and information associated with the relevant email accounts since their creation. (See ECF No. 133-1 at 34 (“warrant *applies to* all information associated with” 5 Google email accounts (emphasis added)); ECF No. 133-2 at 34 (same, as to 3 Microsoft email accounts).) Attachment B provides that Google and Microsoft are “required to *disclose . . .* information to the government for each account or identifier listed in Attachment A for the time period from January 1, 2020 to the present,” and that the government will seize information that falls within a list of 13 categories. (ECF No. 133-1 at 35 (emphasis added); ECF No. 133-2 at 35.) The only attachment requiring disclosure of information—Attachment B—includes a timeframe around the time of the alleged fraud scheme. The Court concludes that with this date

range, the warrants satisfy the Fourth Amendment's particularity and overbreadth requirements. (R&R at 12.) This objection is overruled.

C. Leon Good-Faith Exception

Sharmake Jama also contends that the R&R wrongly applied the *Leon* good-faith exception. "Under the good-faith exception, evidence seized pursuant to a search warrant issued by a magistrate [judge] that is later determined to be invalid, will not be suppressed if the executing officer's reliance upon the warrant was objectively reasonable." *United States v. Houston*, 665 F.3d 991, 995 (8th Cir. 2012) (citation omitted). The inquiry is "confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the [issuing judge's] authorization." *Id.* (citation omitted). The good-faith exception does not apply if, as Jama argues, the warrants were "so facially deficient that no police officer could reasonably presume the warrant[s] to authorize a valid search." *Id.* (citation omitted).

Jama cites *Groh v. Ramirez*, 540 U.S. 551 (2004), to argue that the search warrants were facially deficient because they are not sufficiently particular. He again points to the fact that "*Attachment A* failed to describe any items to be seized at all."⁴ (ECF No. 174 at 6.) He argues that the government's failure to follow *Moulder*, "especially when

⁴ The Court notes that Attachment A does not purport to "seize" any information. *Attachment B* requires the disclosure of information contained in the email accounts identified in Attachment A within a specific timeframe and 13 delineated categories.

Attachment A was devoid of any date range or search terms,” was “problematic to a claim of good faith.” (*Id.* at 7.)

As an unpublished district court case, *Moulder* is not binding authority in this District. And reasonable courts, including this one, disagree as to the validity of these search warrants. *See Bock*, 2025 WL 18629, at *12–14 (collecting cases). The good-faith exception has applied when court decisions conflict on a legal issue. *E.g., United States v. Najarian*, 915 F. Supp. 1441, 1459 & n.16 (D. Minn. 1995) (“Courts have found that the ‘good faith’ exception . . . applies, since the issue presented was sufficiently difficult as to ‘create disagreement among thoughtful and competent judges.’” (citing *Leon*, 468 U.S. at 926)).

The search warrants incorporated Attachments A and B, (ECF No. 133-1 at 39; ECF No. 133-2 at 39), which disclosed the two-step process of the intended searches of particular email accounts within a specific timeframe and 13 delineated categories. Even if Sharmake Jama is correct that the issuing judge wrongly approved the search warrants, the warrants were not so facially deficient that officers could not reasonably presume their validity. The good-faith exception applies. This objection is overruled.

D. Objection to Judge Schultz Hearing the Motion

Finally, Sharmake Jama renews his objection to Judge Schultz presiding over the motion to suppress hearing because Judge Schultz signed the warrants at issue. He cites no authority precluding Judge Schultz from considering the motion to suppress and the

Court is aware of none. He does not describe any prejudice resulting from Judge Schultz hearing the motion. And in any event, this Court has considered the motion to suppress *de novo*. This objection is overruled.

Jama also contends that if Judge Schultz received and reviewed a memorandum that the United States Attorney's Office distributed to the bench advising of the *Moulder* opinion before signing the warrants,⁵ "it would at a minimum, give the appearance of undue influence upon the court, whereby one party is effectively participating in *ex parte* communications on what is sure to be an ongoing Fourth Amendment issue in this district." (ECF No. 176 at 4.) He cites no case law supporting his position and the Court is not aware of any. This objection is overruled.

III. Defendants' Motion to Dismiss for Selective Prosecution

Defendants move to dismiss the Indictment for selective prosecution. They contend that the United States Attorney's Office impermissibly brought this prosecution against them based on their race and ethnicity (Somali or Somali-American and Black).

Courts presume that United States Attorneys "have properly discharged their official duties." *United States v. Armstrong*, 517 U.S. 456, 464 (1996) (citation omitted). Thus, "to dispel the presumption that a prosecutor has not violated equal protection, a

⁵ *Moulder* was issued on Aug. 24, 2022. See 2022 WL 3644893. The warrants were signed three weeks later, on September 15, 2022. (ECF No. 133-1 at 39; ECF No. 133-2 at 39.)

criminal defendant must present ‘clear evidence to the contrary.’” *Id.* at 465 (citation omitted).

To establish selective prosecution, Defendants must show that: (1) they have been “singled out for prosecution while others similarly situated have not been prosecuted for similar conduct”; and (2) “the government’s action in thus singling [them] out was based on an impermissible motive such as race, religion, or the exercise of constitutional rights.” *United States v. White*, 928 F.3d 734, 742–43 (8th Cir. 2019) (citation omitted).

As for the first prong, Defendants must show that they “engaged in ‘similar conduct’ as individuals that [they allege] have not been prosecuted.” *White*, 928 F.3d at 743 (citation omitted). Defendants must present comparators, that is, individuals who: (1) “committed ‘roughly the same crime under roughly the same circumstances’”; (2) “are ‘outside the protected class’”; and (3) “were known to the prosecutor.” *United States v. Lazzaro*, No. 21-CR-173 (PJS/DTS), 2022 WL 16948157, at *2 (D. Minn. Nov. 15, 2022) (citations omitted).

Defendants object to the R&R’s conclusion that no individuals were similarly situated to Defendants. They point to five individuals who “have immediate connections to or are employed by Feeding Our Future,” including three Feeding Our Future board members, who have not been charged. (ECF No. 175 at 2.) They argue that “[t]o assume none of the \$18 million dollars received were used to pay for the wages or salaries of Feeding our Future employees is unrealistic.” (*Id.*) But the selective prosecution standard

is “a demanding one.” *White*, 928 F.3d at 743 (citing *Armstrong*, 517 U.S. at 463). Defendants fail to present facts showing that these individuals participated in the alleged fraud scheme, unlike the Indictment’s factual allegations against Defendants.

Defendants also offer no evidence of racially discriminatory intent by prosecutors. See *United States v. Peterson*, 652 F.3d 979, 981 (8th Cir. 2011) (affirming denial of a motion to dismiss where defendant offered “‘no credible evidence’ that race or gender played a role in the Government’s charging decisions” (citation omitted)). Mere “unsupported speculation and conjecture” does not satisfy Defendants’ burden to “offer ‘credible evidence’ of impermissible motive.” *United States v. Dexter*, No. 21-CR-40 (SRN/BRT), 2022 WL 2965993, at *8 (D. Minn. July 22, 2022) (citing *United States v. Hirsch*, 360 F.3d 860, 864 (8th Cir. 2004)). The government’s indictment of Aimee Bock—who is not Somali or Somali-American and Black—suggests that the government’s decision to prosecute was not motivated by race or ethnicity. *United States v. Bock*, No. 22-CR-223 (NEB/DTS), ECF No. 1 ¶ 24 (alleging Bock “oversaw a massive scheme to defraud”) (D. Minn. Sept. 13, 2022). Defendants fail to overcome the presumption that the government has not violated equal protection. This objection is overruled.

CONCLUSION

Based on all the files, records, and proceedings in this case, IT IS HEREBY ORDERED THAT:

1. Defendants’ objections (ECF Nos. 174, 175) are OVERRULED;

2. The Report and Recommendation (ECF No. 173) is ACCEPTED;
3. Defendants' Motion to Suppress Search Warrant Evidence (ECF No. 132) is DENIED; and
4. Defendants' Motion to Dismiss for Selective Prosecution (ECF No. 135) is DENIED.

Dated: January 17, 2025

BY THE COURT:

s/Nancy E. Brasel
Nancy E. Brasel
United States District Judge